Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

PHISHING PREVENTION USING SERVER AUTHENTICATION

Er. Nancy Girdhar [1] | Dr. Himanshu Monga [2]

1 Dept. of computer Science Engineering, J.C.D.M. College of Engineering, Sirsa, India.

[2] Principal, J.C.D.M. College of Engineering, Sirsa, India.

ABSTRACT

In the modern computer era attacks on systems are increasing. Phishing is one of the serious offenses being committed. In Phishing hacker or group of hackers tries to acquire confidential information such as passwords or bank details etc in an attempt to steal users identity for financial gain or something much worse. In this paper, we are proposing an approach named "Phishing Prevention using server authentication" using which user can check the authenticity of the server with which he is willing to communicate. Here we are using visual cryptography along with general password authentication. In this scheme authentication via images is done. Here the keys being used could be single use keys or one for the time user wants to keep(depending on the will of the implementing party). Under this scheme, the user chooses an image of his will. Then he performs cryptography operation over chosen image and converts it into shares (two at least). User uploads one share onto the trusted server and keeps the other one to himself. The user needs to be attentive while uploading the encrypted share and must upload it only to a trusted server. Whenever the user wants to authenticate the server he asks for the stored share. The server sends the share back to the user after authenticating the user. The user receives the share and performs decryption to obtain the original image. If the image received after decryption is same as original, it implies the server is authentic and the user can proceed with the rest of the transaction.

KEYWORDS: Elliptical Cryptography, Visual Cryptography, Phishing, Security etc.

I. INTRODUCTION

Phishing is an attack executed in order to steal user's confidential information such as authentication details or bank details etc by pretending to be a trusted entity[1]. Such events take place on daily basis. Phishing attacks are carried out by fooling the user, showing him a lookalike of the original web page or by showing him false content. Phishing could also be carried out by email spoofing or instant messaging that may contain the malicious link to a fake website. Phishing could be executed in a plenty of ways[4]. But In all the cases Hacker pretends to be someone he's not (such as a bank helpline). Most of the Phishing attacks are initiated via emails. So a method is being proposed using which phishing attacks could cease to exist. In this method, the web server needs to prove its genuineness before any transaction.

VISUAL CRYPTOGRAPHY:

Cryptography is a technique used to secure our data during transmission; Cryptography uses encryption for securing the data. Encryption changes data to an incomprehensible form that only either the sender or the receiver could decrypt. To achieve these various mathematical algorithms are used.

Visual cryptography was introduced by Naor & Shamir[2]. It provides a secure way to share images. They described visual cryptography as a technique of encrypting the image into shares in a way such that only by stacking a sufficient no. of shares we get the original image back. Each share is a binary image in itself. Here we are using black and white images but the procedure can be implemented using RGB images as well.

There are various implementations of visual cryptography. We are using a basic one in which, firstly the image is converted into a true black and white image. Then a key image of similar dimensions is generated. In this key image, each pixel is randomly set to black or white. Thirdly, the black and white image is encrypted with the help of this key. If the pixel in the key is white then the corresponding pixel in the black and white image is kept as it is else it is flipped(white to black, black to white). This results in two black and white images that have random pixels. Finally, the size of both the images is doubled- each pixel is made into a 2x2 square of pixels. White pixels have white pixels in the top-left and bottom right corners while the remaining two corners are made black, similarly, a black pixel is turned into an opposite 2x2 square. These are the two final shares. When these two shares are made to overlap transparently then the black and white image is produced[3]. It happens because of the difference of black pixels in key and the encrypted image. When overlaid all the four squares of a black pixel become black while the white pixels remain same in both of the resultant and the encrypted images. Hard copies printed on transparent papers can also be made to overlap to get the original image.

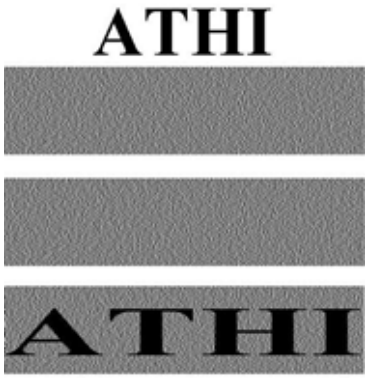

Fig 1 : A visual example of Visual Cryptography

Figure shows the application of visual cryptography on an image. Firstly the image is being converted into two share, and then these shares are being overlaid to reproduce the original image.

Elliptical Curve Algorithm:

Elliptical curve cryptography is a public key encryption scheme[6]. As we know public key encryption schemes are mostly based on a mathematical operation that is easy if we know some certain things but it is very difficult if we don't have that particular knowledge. These certain things accomplish the purpose of the secret key. Elliptical curve algorithm is such an algorithm. Elliptical curve algorithm depends upon "Elliptic Curve Discrete Logarithm Problem"[6]. Elliptical curve cryptography was invented independently by Neal Koblitz and Victor S. Miller in 1980's. Many cryptography algorithms like ElGamal scheme or Diffie Hellman algorithm could be adapted to use principles of ECC. The main advantage of using ECC is its usage of small key sizes[6].

Elliptical curves:

Mathematically elliptic curves are defined as plain algebraic curves satisfying the equation:

$$Y^2=X^3+ax+b$$

It's graph has no self-interactions or cusps[6]. It means that this is non-singular. The graph for elliptic curve looks something like:

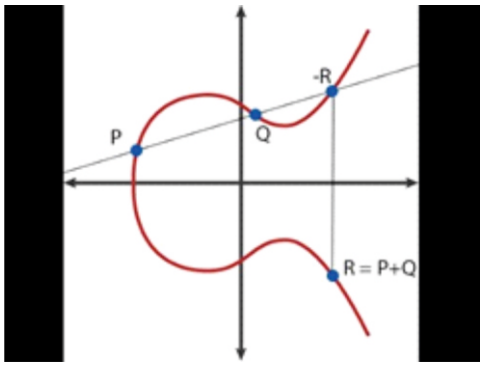

Fig 2 : Shows the general structure of an elliptic curve

An elliptic curve is a curve over a finite field, consisting of points satisfying the elliptic curve equation(one mentioned above) along with an acclaimed point at infinity. This point at infinity is denoted by ∞[8].

If there are no repeated factors for the curve equation then this curve could be used to form a group. A group over an elliptic curve is a set of points on the curve. When we add up points from the same group the resultant is a point belonging to the same group[8]. To perform cryptography, all points under consideration must have whole numbers as coordinates. The main trick behind elliptic curve cryptography is the presence of all multiples of the point taken for cryptography operation on the curve itself.

Generating Public and Private Keys:
First of all the elliptical curve for the cryptography purpose is chosen(both the participants must agree on the curve, they must be aware of its equation). Then they agree to a point 'F' on this curve. This can be executed in the presence of an intruder. Then Alice(Let's call one user Alice and other Bob) picks a random number 'ASeck'(Not necessarily a point on the curve)and then he computes 'APubKey=ASecK*F '. Because of being a multiple of 'F' 'APubKey' lies on the curve. 'APubKey' is user's public key and 'ASecK' is user's secret key. Similarly, Bob computes his public key say 'BPubKey' and his secret key say 'BSecK'.

Encryption and Decryption:
Now Alice and Bob both can compute a key using each other's public keys. Bob can calculate this key by multiplying his secret key with Alice's public key and similarly Alice can calculate this key by multiplying his secret key with Bob's public key. This key will be equivalent to:

$$CSecK = ASeck*BSeck*F$$

Both the participants can calculate this Common Secret Key after exchanging their public keys. The intruder will never be able to compute this because of the absence of secret keys[7].

Now Sender encrypts using receiver's public key and receiver decrypts using his private key.

The intruder say Eve, will need to compute at least one secret key. This computation of the secret key from public keys and the point is called 'dynamic logarithm problem of finite fields' which takes a lot of time to solve if a curve of sufficient order is used.

Encryption :
Let 'm' be the message that is to be exchanged, and 'M' is its corresponding point on the curve. K is a randomly selected number from (1,n-1). Two ciphers will be generated as:

$C1 = k*P$

$C2 = M + k*Q$

Now both the ciphers are transmitted.

Decryption :
Firstly we will calculate the point on the curve

$$M = C2 – d * C1$$

Now this point can further be translated into message.[9]

Ongoing Procedure:
There are flaws in the current methodology that leave users as preys to the hackers. Hackers might steal user's information by phishing or some other methods taking advantage of these flaws. Under ongoing procedure user's confidential information is obtainable at the time he logs in. And after collecting the information to clear user of any doubt he could be directed to the original website. Thus ongoing procedure has some serious issues that need to be dealt with[5].

Recommended Procedure:
Using the proposed technique one can test the website for its authenticity. Thus the data exchange would only take place between the trusted servers and the user. This technique has three phases:

1) Image Uploading And Keys Generation:
Websites can store image shares that could be used to assure the user of the authenticity. The user chooses an image, applies visual cryptography to create image shares. One of the shares is sent over to the trusted server and the other is kept by the user. This can be done at any time such as during registration phase or any other time whenever the user wants to enhance security. The image used could also be changed at any time user feels like there's a breach in security. The user also generates keys for the implementation of elliptic curve cryptography.

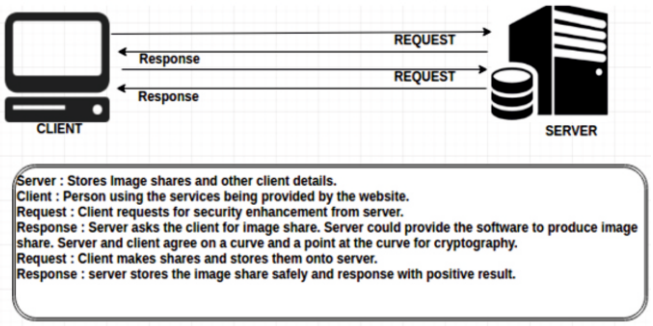

Fig 3 : Image share storage at server side

2) User's authenticity test:
Now, whenever the user is asked for information by the website he can check for the authenticity of the seeker. But before that, he needs to prove his authenticity to the user. For that, he needs to provide his unique user identification and pass the captcha (a computer program or system intended to distinguish human from machine input).Now if the server under suspicion is a poser then it'll have to ask the original server for user's previously stored image and in order to get that it'll have to pass the captcha. Hence Trusted server can verify that the request has been generated by a bot and not a human and thus refrains from sending. If the user requests to the original server, the user can pass the captcha that bot or fake server failed to do. In this manner, the server verifies the authenticity of the user.

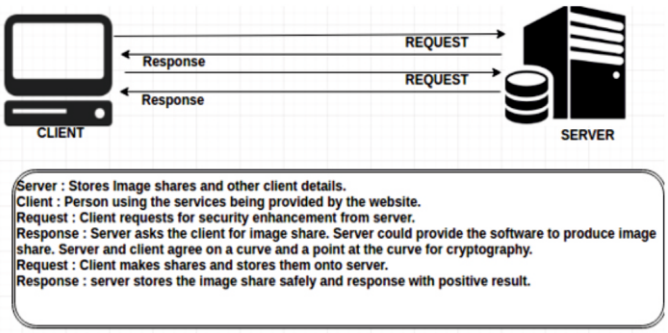

Fig 4 : Client Authentication By Server

3) Server's Authenticity Test:
After the server has verified the authenticity of the user then it transmits the stored share of image encrypting using the key it obtained with the request. On receiving the image share user decrypts the image share using his private key and overlaps the received share over the other share that he kept during the registration. If the original image is retrieved then the server is authentic else it could be a fraudulent bot. In this manner, the user can verify the authenticity of the server.

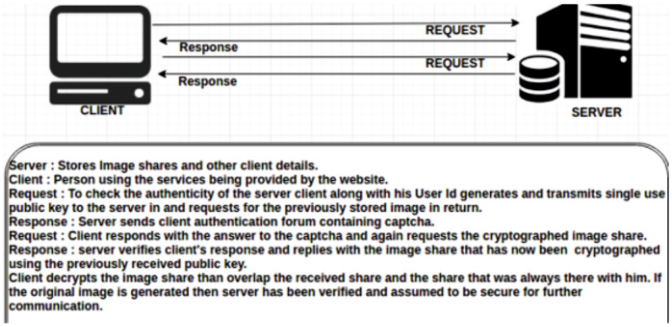

Fig 5 : Server Authentication By Client

Implementation:

The aforementioned system could be implemented using J2EE(Java 2 Platform, Enterprise Edition) or any other Web development languages such as PHP, ASP.net etc. But we have implemented that system using J2EE. Here we've shown the approach using flowchart and some visually encrypted images. And when this system is compared to older systems it proves to be efficient in the manner of being more secure and versatile.

Conclusion:

As the internet usage increases so do the attacks to steal important data. Thus we need more sophisticated systems to comprehend the security aspect. Systems implemented using this approach are more secure because of the fact: decryption can only happen with the private key of the user and as keys could be made single use it makes things even worse for the hackers. Also, the user can change the stored image anytime making it even more secure. This idea could benefit all the websites that deal with confidential information, as it provides the essential extra security required.

REFERENCES:

1. Ollmann G., the Phishing Guide Understanding & Preventing PhishingAttacks, NGS Software Insight Security Research.
2. M. Naor and A. Shamir, Visual cryptography, in Proc. EUROCRYPT, 1994,pp. 1–12 .
3. B. Borchert, .Segment Based Visual Cryptography, WSI Press, Germany, 2007.
4. A literature survey on social engineering attacks: Phishing attack.Surbhi Gupta; Abhishek Singhal;Akanksha Kapoor 2016 InternationalConference on Computing,Communication nd Automation (ICCCA) Year: 2016.
5. Aboli bhanji, Priyanka jadhav, Sayali Bhujbal, Punam Mulak, Secure ServerVerification By Using RSA Algorithm And Visual Cryptography in IJERT, 2013.
6. Soram Ranbir Singh, Ajoy Kumar Khan,Takhellambam Sonamani Singh, A Critical Review on Elliptic Curve Cryptography, IEEE Conference, 2016.
7. Omkar Guru et al., NIT Rourkela, 2007
8. Megha Kolhekar, Anita Jadhav, Implementation of Elliptic CurveCryptography On Text And Image,IJECBS 2011
9. Fatema Akhter, A Novel Elliptic.Curve Cryptography Scheme Using dom Sequence.